REMARKS

Response to Arguments

The examiner withdrew the double patenting rejection as to co-pending applications 10/701,154; 10/701,353; 10/701356 and 10/701,404 as these co-pending applications are not yet ready for allowance.

The examiner also withdrew the rejection under 35 U.S.C 101.

However, Examiner maintained the double patenting rejection with respect to allowed co-pending application 10/701,376 (now US Patent 7,363,656) and the rejection of the claims as anticipated by Gupta.

Double Patenting

The examiner rejected Claims 1 - 33 on the ground of non-statutory obviousness-type double patenting as being unpatentable over amended claims 1-5, 7-9, 11-16 and 18-21 of co-pending application 101701,376.

The examiner is kindly referred to the office action for the complete text of the rejection.

Claim 1 of the '656 patent is reproduced below:

> 1. A computer implemented method for detecting conditions in a network, comprising:
> finding anomalies, which are low-level differences in network operation relative to some comparison period, by:
> producing a moving average of a parameter associated with network packet flows;
> determining whether a variance in the parameter exceeds a threshold;
> traversing a connection table that maps each host to a "host object" that stores information about all traffic to or from that host to determine connection patterns of a particular host in the network, and if the variance exceeds the threshold to indicate an anomaly,
> identifying and correlating anomalies from the connection patterns with other found anomalies that exceed the threshold into at least one operationally relevant event indicating a detected event in the network.

Claim 1 of the present application is reproduced below, and in contrast claims:

> 1. (Previously Presented) A computer implemented method comprising:
> retrieving connection pairs from a connection table for a host that is attempting to gain access to another host in a networked computer system;
> determining whether that one host attempting to gain access has accessed the other host previously; and if that one host has not accessed the other host previously,
> determining if other anomalies in the connection patterns of each host exist to establish an event severity level indicating a likelihood that the host attempting to access another host is attempting an unauthorized access.

While each of the claims makes use of the novel connection table, the claims do so in different, patentably distinct manners and define patentably distinct arrangements.

Claim 1 of the '656 patent finds anomalies by, producing a moving average of a parameter and determining whether a variance in the parameter exceeds a threshold. Claim 1 requires the method traverse a connection table and identify and correlate anomalies in connection patterns with other found anomalies that exceed a threshold into an operationally relevant event. Contrast that with claim 1 of the present application which requires retrieving connection pairs from the connection table for a host attempting access to another host, and determining whether the host attempting access has accessed the other host previously … .

Claim 1 of the '656 patent neither describes nor suggests at least the feature of "determining whether the host attempting access has accessed the other host previously" whereas claim 1 of the present application neither describes nor suggests at least the features of "producing a moving average of a parameter and determining whether a variance in the parameter exceeds a threshold."

The examiner takes the position that the feature of instant claim 1 is merely a difference in wording and further argues that: "… regardless of the wording, still maps to "**traversing a connection table that maps each host to a "host object" that stores information about all traffic to or from that host to determining connection patterns of a particular host in the network.**"

Applicant readily acknowledged that both claims access the novel connection table. However, while claim 1 of '656 patent recites "identifying and correlating anomalies from the connection patterns with other found anomalies that exceed the threshold into at least one operationally relevant event indicating a detected event in the network", claim 1 of the present case requires "determining if other anomalies in the connection patterns of each host exist . . . ." Thus, present claim 1 requires finding two anomaly types. One anomaly type is new connections for a host attempting to gain access to another host, and the other type is any other anomalies in the connection patterns of each host.

The examiner also incorrectly reasons that: "**it is still determining anomalies and the language co-pending claims describes the structure of determining anomalies that will be used to "detecting unauthorized access in the computer network.**" Applicant responds that the examiner has merely provided a naked conclusion that the co-pending dependent claims describe the structure of detecting unauthorized access. The examiner has not provided any reasoning to support this contention. Applicant contends that this contention is erroneous.

The examiner erroneously concludes that: "**Therefore, the main, and arguably only, difference in structure used make the determination about authorized access and/or unauthorized access, while the instant claims are broadly claiming the detection and determination of anomalies in the connection pattern, the copending claims are more specific as to the structure of "producing a moving average of a parameter associated with network packet flows" (please refer to 10/701,376 paragraph [0068 -0071], it merely consist of a substitution of what is used to make that determination.**" Applicant disagrees. The claims do not suggest merely a substitution of what is used to make the determinations, for the reasons pointed out above.

Moreover, even if this were true, which Applicant does not concede, the examiner needs to show that these "mere substitutions" are obvious from the claims. That is, even the presence of differences in claimed details is generally sufficient to overcome an obviousness-type double patenting rejection.[1] Accordingly, this rejection is improper and should be removed.

35 U.S.C. § 102

The examiner maintained the rejection of Claims 1-33 under 35 U.S.C. 102(e) as being anticipated by Gupta et al. (7,234,168). The examiner stated in response to Applicant's prior Reply:

[1] See *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970).

... the applicant argues that the prior art Gupta et al. (Patent 7,234,168) does not disclose or suggest "retrieving connection pairs from a connection table for a host that is attempting to gain access to another host". This argument is not persuasive.

Gupta et al. teaches "an anomaly detector (62), which is used to identify network traffic anomalies indicative of an attack, and is implemented to create a characterization of the normal behavior of the system and detects anomaly for the observed packets based on the characteristics". Furthermore, Gupta teaches "The anomaly detector detects crafted packet attack or DDOS attacks based on the normal traffic profile of a target domain, which may be a single host/server, a sub-net, or an enterprise network" (See Gupta column 6 lines 3 - 42 and Column 7 lines 10 - 60).

Examiner further points out that "retrieving connection pairs from a connection table for a host that is attempting to gain access to another host" is not the heart of the invention. If the applicant has the special method of retrieving connection pairs from a connection table then the examiner suggests amending the claims to explicitly recite such a retrieving technique.

A recitation directed to the manner in which a claimed apparatus is intended to be used does not distinguish the claimed apparatus from the prior art if prior art has the capability to do so perform (See MPEP 21 14 and Ex Parte Masham. 2 USPQ2d 1647 (1987)). The prior art is replete with references disclosing "retrieving connection pairs from a connection table for a host that is attempting to gain access to another host". (See PTO 892).

Examiner also points out the instant invention is well depicted in Gupta Fig.2 and 3, Column 4 line 15 - Column 8 line 40 and Column 10 line 22 - Column 11 line 35, wherein Gupta teaches "determining other anomalies includes determining whether previous connection patterns of the hosts indicate that the hosts are in roles that are not normal for the hosts" see Gupta Column 6 lines 12 - 55 and connection patterns" (also, see above arguments supporting these additional limitations. Examiner maintains the rejection of Claims 1-33.

The examiner is kindly referred to the office action for the complete text of the rejection.

Claim 1 includes the features of: "... retrieving connection pairs from a connection table for a host that is attempting to gain access to another host ... and if that one host has not accessed the other host previously, determining if other anomalies in the connection patterns of each host exist to establish an event severity level indicating a likelihood that the host attempting to access another host is attempting an unauthorized access.

The examiner argues that: "**"retrieving connection pairs from a connection table for a host that is attempting to gain access to another host" is not the heart of the invention.**" Applicant is unaware that inventions had hearts, but maintains that the feature is novel over the cited art. Claim 1 includes a novel feature of retrieving connection pairs from a connection table.

The examiner argues that this feature is a mere intended use. Applicant disagrees. Claim 1 does not recite a mere intended use but positive steps that are neither described nor suggested by the cited art and in particular Gupta. The examiner also states: "**The prior art is replete with references disclosing 'retrieving connection pairs from a connection table for a host that is attempting to gain access to**

another host'." Applicant disagrees and specifically challenges the examiner to cite prior art to support this contention. So far the examiner has not done so.

Gupta neither describes nor suggests at least the foregoing features of claim 1. The examiner continues to argue that: "**Gupta teaches "retrieving connection pairs from a connection table for a host that is attempting to gain access to another host."** The examiner however still has not provided any specific cite to this or to any of the other features of claim 1, but merely gives a cite at the end of the argument to "**(Column 6 lines 3 - 42 and Column 7 lines 10-60).**"

At that passage, Gupta neither describes nor suggests "retrieving connection pairs from a connection table for a host that is attempting to gain access to another host ... ." At **Column 6 lines 3 – 42** Gupta discusses anomaly detection and signature analysis. Signature analysis involves finding known patterns in packets,[2] whereas anomaly analysis according to Gupta involves a characterization of the normal behavior of the system.[3]

While claim 1 includes features of anomaly detection, claim 1 also requires the feature of retrieving connection pairs and determining whether one host has accessed another host previously. The combination of these features of using connection patterns of hosts to determine whether "one host has not accessed the other host previously" is neither described nor suggested by Gupta.

The examiner also argues that Gupta teaches: "**determining whether that one host attempting to gain access has accessed the other host accessed previously;** Gupta mentions unauthorized access and access to hosts. However, Gupta does not mention determining whether one host has attempted to access the other host previously and to use this determination to ascertain whether other anomalies exist in connection patterns to warrant raising the severity of an event.

In reply to the previous action, the examiner argues that: "**... the instant invention is well depicted in Gupta Fig.2 and 3, Column 4 line 15 - Column 8 line 40 and Column 10 line 22 - Column 11 line 35, wherein Gupta teaches "determining other anomalies includes determining whether previous connection patterns of the hosts indicate that the hosts are in roles that are not normal for the hosts" see Gupta Column 6 lines 12 - 55 and connection patterns" (also, see above arguments supporting these additional limitations.**" The examiner now refers to additional passages from Gupta, but these additional passages from Gupta still neither describe nor suggest the claimed invention.

---

[2] Gupta see generally discussion starting at col. 11 line 57.
[3] Id. Col. 6, lines 37-38

The examiner points to Figs. 2 and 3, but nothing specifically in those figures. Fig. 2 illustrates a network security sensor and Fig. 3 illustrates processing steps performed by the network security sensor. Neither Fig. 3 nor Fig. 3 suggests the features of claim 1. The examiner points to "**Column 4 line 15 - Column 8 line 40 and Column 10 line 22 - Column 11 line 35**" as teaching connection patterns and roles (feature of claim 2).

From Col. 4, line 15 to Col. 6, Gupta principally discusses signature analysis. From Col. 6, line 11 to Col. 8, line 40, Gupta discusses "anomaly detection." However, throughout the discussion on anomaly detection Gupta describes building a measure of normalcy and measures of discrepancy. Gupta fails to suggest however "retrieving connection pairs from a connection table for a host that is attempting to gain access to another host in a networked computer system, determining whether that one host attempting to gain access has accessed the other host previously ... ." Continuing with Gupta, at Col. 10, line 2 to Col. 11, line 35 Gupta discusses application anomalies through system connectivity profile checking, which involves defining various vectors as set out in Col. 10, lines 29-34, but again is silent on the claimed features.

Accordingly, claim 1 and claims 12 and 23 which include analogous features as claim 1 are neither described nor suggested by Gupta.

As for Claims 2, 13 and 24, at least because Gupta neither describes nor suggests connection patterns of the hosts, and therefore Gupta cannot suggest: "determining other anomalies includes determining whether previous connection patterns of the hosts indicate that the hosts are in roles that are not normal for the hosts." Indeed, neither at the cited passage (Column 7 lines 29-45) nor elsewhere does Gupta suggest roles, much less using roles of hosts in conjunction with connection patterns to determine other anomalies.

Similarly, Claims 3, 14, and 25; Claims 4, 15, and 26; Claims 6, 17, and 28; Claims 7, 18, and 29; and Claims 11, 22, and 33 all of which either directly or indirectly rely on the connection table and/or connection patterns thus further distinguish over Gupta, because as set forth above Gupta does not suggest a connection table or processing based on connection patterns in detection of anomalies.

Claims 9, 20 and 31, which requires roles further distinguishes over Gupta, because as set forth above Gupta does not suggest using roles in detection of anomalies.

Claims 5, 16 and 27; Claims 8, 19 and 30; and Claims 10, 21 and 32 are allowable at least for the reasons discussed in their respective base claims.

It is believed that all the rejections and/or objections raised by the examiner have been addressed.

In view of the foregoing remarks, applicant respectfully submits that the application is in condition for allowance and such action is respectfully requested at the examiner's earliest convenience.

All of the dependent claims are patentable for at least the reasons for which the claims on which they depend are patentable.

Canceled claims, if any, have been canceled without prejudice or disclaimer.

Any circumstance in which the applicant has (a) addressed certain comments of the examiner does not mean that the applicant concedes other comments of the examiner, (b) made arguments for the patentability of some claims does not mean that there are not other good reasons for patentability of those claims and other claims, or (c) amended or canceled a claim does not mean that the applicant concedes any of the examiner's positions with respect to that claim or other claims.

This Reply is accompanied by a Notice of Appeal.

Please charge the Petition for Extension of Time fee of **$60** and please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 6/1/07

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (877) 769-7945